IDNewswire
Trends in Personal Identification and Biometrics
www.cardtechnology.com
Vol. 2 No. 1 January 8, 2003

Can Smart Cards Play The Biometric Match Game?

In these times of heightened security, several government agencies and private companies are considering storing a biometric identifier, which verifies the identity of the cardholder by a unique physical characteristic, on their employee ID cards.

The biometric data could replace personal identification numbers, which are difficult for cardholders to remember or can be stolen. The data could also be used in conjunction with a PIN to provide what many experts consider to be a very high level of security, three-factor authentication, which is something you have — the card; something you know — your PIN; and something you are — your fingerprint.

ID issuers would like the biometric identifier to have the same functionality as a PIN, meaning that the smart card's microprocessor could match the biometric data, or template, stored on the card with the live image taken off the biometric sensor. Doing the match on the card provides greater privacy to the cardholder because the biometric data stays in the secure environment of the smart card. In addition, having the smart card make the match eliminates the need for secure access to a personal computer or server to crunch the matching algorithms.

At this point, however, match-on-card technology remains more of a theory than a tried-and-true option for issuers. There are a handful of match-on-card deployments, including the Dutch Ministry of Justice, which has issued 15,000 employees an ID card used to securely log onto its computer network. But many industry insiders are keeping tabs on the U.S. Department of Defense, which is testing match-on-card technology for its Java Card-based Common Access Card. By last fall, the agency had issued 1 million of the 4 million Common Access Cards it plans to issue to active-duty military personnel, some Reservists and National Guard, as well as the DOD's civilian employees and eligible contractors.

U.S. agencies such as the Transportation Security Administration, which potentially may issue 12 million cards to airport and seaport workers across

> **Match,** Page 2

Facial Recognition Catching Fraudsters In Illinois

Ruby Haywood had eight Illinois driver's licenses; nevertheless, state officials determined it wasn't because she liked to drive. Although Haywood's photograph had appeared on all the licenses, each had a different name and address.

Illinois uses facial recognition biometrics to check the identity of those renewing license or ID's.

Enforcement agents from the office of the Illinois Secretary of State, the state's driver's license issuer, discovered that Haywood had used the licenses and five other pieces of official identification from other states to perpetuate an identity fraud scheme bilking 13 individuals, including a 93-year-old woman, out of $280,000. In July, the 69-year-old Haywood plead guilty to identity fraud, and was sentenced to a four-year prison term.

So how did the Illinois Secretary of State find out that Haywood's face belonged on a wanted poster rather than on an Illinois driver's license? By using facial-recognition biometrics.

In 1999, the Illinois Secretary of State's office became

> **Illinois,** Page 3

How Do You Know If It's A Real Finger?

Spoofing is the term commonly used for tricking or hacking biometric systems.

Last May, a Japanese mathematician was able to fool 11 fingerprint scanners 80% of the time using fingers made out of gelatin. Later on, reporters at a German technology magazine were successful in spoofing iris and facial recognition systems using high resolution images of faces and irises, the colored part of the eye.

While these attacks are cause for concern, biometric vendors and analysts say they can be avoided by the proper use of technology, combined with appropriate security procedures.

The U.S. Department of Defense, which plans eventually to deploy thousands of biometrics devices, is working with vendors to stop spoofing by using liveness detection.

Liveness detection makes sure that the individual presenting the biometric is actually at the device. For example, with facial recognition someone would have to blink or smile at the camera to show that it's not a picture being presented, says Frances Zelazny, communication director with Identix Inc, a fingerprint and

> **Spoofing,** Page 4

Familiar Voice Unlocks Services

Voice Recognition is likely to grow rapidly because of its ease of use with mobile and hard-wired telephones. The International Biometric Group provides some insight in the Research Corner.

> **Voice,** Page 5

Medical Museum Safeguarded With Hand Geometry

Hand geometry is being used for access control at the New York Weill Cornell Medical Center museum and library.

> **Museum,** Page 3

> Match, Page 1

the country, will likely model itself after the CAC card, says Powell Benedict, a technical consultant for Minnetonka, Minn.-based biometrics firm Identix Inc. "The DOD has invested a lot of time and money in its CAC card, and many other potential users will follow its lead," he says.

But more testing, like the DOD's, needs to be done on the technology before issuers are sure that a smart card microprocessor, with its limited processing power, can accurately match the templates as well as a computer in an acceptable time of 2 seconds or less. "There is much less processing power available in a smart card compared to a reader or PC," says Kush Wadhwa, a senior consultant at the New York-based International Biometric Group. "The matching algorithm may need to be simplified in order to ensure an adequate response time, and that could affect accuracy. But more testing is required to be certain."

Today, most of the match-on-card systems use fingerprints as the biometric identifier. In part, that is because it is the maturest of biometric technologies, says Raymond Makewell, head of research and development for Australia-based Keycorp's smart card group. Several smart card vendors, including U.S.- and France-based SchlumbergerSema, France-based Gemplus International SA, and Fremont, Calif.-based ActivCard, have teamed up with biometric vendors such as Sweden-based Precise Biometrics or Identix to use their fingerprint recognition software.

These vendors offer match-on-card using smart cards with their own operating systems, as well as with platforms such as Java Card, which are available from multiple vendors. In addition, Keycorp is working with Precise to offer match-on-card technology on smart cards using the Multos operating system, another "open" platform available from multiple vendors.

'We were able to successfully apply match-on-card technology … but it was not capable of being done before three months of work.'
– Bob Wilberger, Northrup Grumman

But the system must be tweaked in order to offer match-on-card on the standard microprocessor cards. Most smart cards do not have the processing capability to handle match-on-card within acceptable time limits. Smart card vendors normally split the processing between the card and a reader or PC, so a match can be made in about 2 seconds.

With most match-on-card systems, the image taken from the sensor is sent to a preprocessing unit to extract the data from the live image that corresponds to the stored template on the smart card. The preprocessed template is then sent to the smart card to do the match.

Sweden-based Precise Biometrics is among the fingerprint vendors that offers users a match-on-card capability.

Another problem issuers must contend with is that biometric vendors' software is proprietary. This means that if issuers want to store more than one biometric algorithm on the card, such as one for fingerprint and another for iris, it would have to create a biometric-enabled software application, or applet, for each algorithm.

Java Card vendors have addressed this problem by creating a software application that sits between the applet and the biometric algorithms stored on the chip. The software, known as an application programming interface, translates the biometric algorithms' commands to the Java Card applet, enabling issuers to store more than one type of biometric algorithm on a Java Card without having to write an interface for each one. The API also enables issuers to use Java Cards from multiple smart card vendors.

The U.S. Department of Defense tested match-on-card technology using the Java Card Biometric API last summer, with positive results, says Identix's Benedict. "Our algorithm, written in Java, took from 1 second to 2 seconds to do the match," he says. Northrup Grumman used Identix's fingerprint algorithm and readers for its match-on-card tests. The DOD also contracted McAllen, Va.-based BearingPoint Inc., formerly KPMG Consulting Inc., for testing.

The DOD tests showed that match-on-card technology works, says Bob Wilberger, Northrup Grumman's director of smart card initiatives. "We were able to successfully apply match-on-card technology in a time frame that was acceptable, which was 2 seconds," he says. "But it was not capable of being done before three months of work. That's how long it took for us to move the algorithms to the smart card itself so we could do the match."

Identix and Northrop Grumman shrunk the fingerprint-matching algorithm down to 1,800 bytes and the biometric template to 250 bytes, says Benedict. Despite the fact that Identix had to strip out functionality in the algorithm, which increases the chances of an inaccurate match, in the case of DOD tests, the accuracy rates remained at 99%, the same as before, says Identix's Benedict.

In addition to testing match-on-card technology, Northrup Grumman and BearingPoint are testing putting the biometrics on a central database, a local database, or on a specific personal computer. The DOD has not made any decisions on how it will store the biometrics at this time, or whether it will use match-on-card technology, says a BearingPoint spokesperson.

Match-on-card technology provides some promising benefits to issuers, but too many unknowns about the technology's performance could leave card issuers hesitant to deploy it at this time. The need for secure physical and logical access systems, however, is likely to spur vendors and issuers to conduct the testing necessary to make match-on-card technology a viable option. <

> Illinois, Page 1

the country's first driver's license issuer to employ facial-recognition biometric technology to identify people with multiple driver's licenses as part of its fraud-fighting efforts. And more states are jumping on board with the biometric, including Colorado, North Carolina, West Virginia and the District of Columbia. Facial recognition vendors add that most states looking to upgrade license systems are investigating facial recognition.

"We wanted a strategy to reduce fraud by eliminating multiple identities in our database," says Beth Langen, the Illinois Secretary of State's division administrator for policy and programs.

Littleton, Mass.-based Viisage Technology Inc. installed the facial recognition system Illinois uses. Viisage loaded its software on the Secretary of State's computer system to determine whether driver's license applicants had one or more licenses in its database, Langen says.

When a motorist applies for a new Illinois license, or renews an existing one, Secretary of State employees take a digital photograph of the person. The state employee immediately gives the individual their driver's license that is mounted on white-plastic card stock, similar to the plastic used in credit cards.

The facial recognition software then searches the Secretary of State's database to determine whether the applicant's face matches the faces of others with driver's licenses in the database. The Secretary of State manages a 13 million-person database, but not everyone is a motorist. Some have non-driver's license state identification cards, Langen says.

If the individual has more than one driver's license on file, the Secretary of State's office writes a letter notifying them that they are under investigation, Langen says.

Viisage software works by translating the motorist's face into a unique string of numbers. "It looks at baseline facial features, such as a person's eyes being farther apart," says Cameron Queeno, Viisage's marketing director.

So far Viisage has helped Secretary of State's Office catch 1,000 individuals with multiple driver's licenses, says Langen. She admits that's not a huge number. But Queeno says it's very important considering the driver's license vaunted role in America.

"It's closest thing we have to a national identification card," Queeno says."The police may ask you to produce your driver's license once or twice in your lifetime, but people will constantly ask you to produce your driver's license as proof of identification to cash a check. By catching people with multiple licenses, the state is reducing the chances that they may commit fraud."

Joan Vecchi, Colorado's director of driver control, which began employing facial biometric technology in October, adds that the Colorado Attorney General estimates that a person with a false driver's license writes, on average, $5,000 worth of bad checks.

Up until now driver's license facilities have relied on what is known as "text stream," an individual's name, address and Social Security number, along with other data to help identify them. However, text stream doesn't always work because someone can try walking into a license issuing facility with somebody else's information and possibly receive a license for illegal purposes.

The Sept. 11 terrorist attack and well-publicized identity-fraud cases also have increased interest in facial recognition biometrics by driver's license-issuing agencies, says Jay Maxwell, chief information officer at the American Association of Motor Vehicle Administrators. Maxwell cautions, however, that facial recognition biometric technology is a work in progress.

"It's an improvement over what we have today, but it's still a back-end system," Maxwell says. "States should not use it in the front end to deny applicants driver's licenses based on the results of facial biometric-recognition technology. Once facial recognition-biometric technology identifies a person who may have more than one driver's license, state employees should study the photographs to make sure it's a correct match."

Colorado's Vecchi agrees with Maxwell, saying the system is not foolproof. Vecchi's department is using Digimarc ID Systems LLC's facial-recognition biometric system to eliminate driver's license fraud. The Colorado Legislature had mandated that the state take steps to prevent individuals from obtaining multiple licenses.

Although Digimarc has helped Vecchi's department uncover two fraudulent driver's license applications a week, including identifying men who applied for driver's licenses dressed as women, it has had some problems as well – identifying blacks as being white and vice versa, Vecchi says. "If you saw a white woman and a black woman walking down the street, you would know they were not the same person, but the Digimarc system doesn't know that," he says.

Peter Edelstein, Digimarc's senior marketing manager, says the company's system does not look at skin color, makeup, or gender. "It creates a mathematical template of the face, weighted to the eyes, cheek bones, nose and mouth," Edelstein explained.

Learning how to use the system correctly has been a bit of trial and error in Colorado. Initially, state employees ran each photo through the 10-million image database requesting any stored image photos that matched with a 50% reliability rate. But the number of matches was overwhelming. "There were so many photographs that it was unworkable," Vecchi says. "We now request an 80% match." <

New York Medical Museum Uses Hand Geometry Scanners

IR Recognition Systems, the biometric subsidiary of Ingersoll-Rand and a provider of hand geometry readers, announced Tuesday that its reader is providing access control to the private library and museum at the New York Weill Cornell Medical Center. The library and museum are so secure that it is only accessible to 12 people. The library contains equipment that was used for patient treatment and research articles on psychiatry. Users enter a personal identification number and then place their hand on the scanner for entry into the museum. Ben Scaglione, director of security at New York Weill Cornell Medical Center, says the hospital is planning on installing additional scanners to secure its utilities. The hospital currently uses a magnetic-stripe ID card system, he says. <

DOD, ING Orders Identix Readers

The U.S. Department of Defense has ordered 450 of Minnetonka, Minn.-based Identix Inc.'s single-fingerprint readers. Wilmington, Del.-based ING DIRECT, a bank offering financial products to customers over the Internet and telephone, also purchased several fingerprint scanners. The Pentagon's readers will be used for personnel fingerprint enrollment and verification applications. ING's systems will be installed at its headquarters, as well as its Los Angeles, and St. Cloud, Minn., offices to perform employee background checks. <

Corrections Dept. Goes with Saflink

Bellevue, Wash.-based Saflink Corp. announced a 3,000-user site license for its biometric security software from the Minnesota Department of Corrections. The

> Briefs, Page 4

> Spoofing, Page 1

facial recognition vendor.

With a fingerprint scanner it's the way an individual may place their finger on the scanner. "If it's exactly the same minutia points that were presented during enrollment there's probably a problem," Zelazny says. During enrollment a user typically has a minimum of three scans taken of the finger. The minutia captured during a livescan is "never the same minutia that's presented at enrollment," she says.

The Defense Department's Biometric Fusion Center, which tests biometric devices, is looking at how biometrics can be layered with personal identification numbers, or tokens, such as smart cards, says a center spokesperson. Layering biometrics with a smart card means the individual trying to gain access would have to present the biometric and smart card to gain access. Just spoofing the biometric would not be sufficient.

The Pentagon is focusing its anti-spoofing efforts in the areas where it would be most needed, such as in the battlefield, says Greg Johnson, technology spokesperson at the Biometric Management Office, the organization overseeing biometric efforts for the DOD.

"Comparing biometrics to physical security, nobody is going to put a $10,000 foolproof lock on a $300 bicycle when a simple bike lock will do," Johnson says. "If a serious threat of spoofing warrants precaution towards a particular biometric security device, then action will be taken to address the issue."

Biometric vendors say they have spent considerable time trying to spoof their own devices, but they are reluctant to be specific for fear they will give too much information to possible spoofers.

Sherman Oaks, Calif.-based Bioscrypt Inc.'s engineers spent several weeks working with different types of molding materials trying to spoof fingerprint sensors after the Japanese attacks, says Robert Gailing, marketing manager at Bioscrypt. He says the attacks failed.

Iridian Technologies, the patent holder on iris biometric systems, has a team of researchers devoted to evaluating threats and developing countermeasures against spoofing, says Lina Page, director of global marketing at Iridian.

While vendors work on ways to improve technology to stop spoofing, analysts and systems integrators recommend having security policies that would prevent the attacks.

Tim Corcoran, senior systems engineer for biometrics at Northrop Grumman IT, says proper procedures are needed to go along with any biometric system. Northrop Grumman is a systems integrator that has been testing biometric devices for the Pentagon.

If an area requires very high security, organizations should think about guards or video surveillance to make sure devices are not tampered with. "It's a combination of things you can do to deter attempts," Corcoran says. "If all you've done is build a ranch on biometrics, you haven't built a very good ranch."

Northrop Grumman would not suggest a security system with just biometrics, Corcoran says. The company recommends using a card along with a biometric. This would require intruders to need both the biometric and PIN or other token.

Organizations can also set the devices to spot certain anomalies, such as an employee trying to use a device at an abnormal time, Corcoran says. If something out of the ordinary is detected, security could be notified.

The International Biometric Group also has some suggestions on ways to stop spoofing of biometrics. First the group recommends randomizing verification data. For example, when enrolling a user might submit three fingerprints, or possibly two distinct voice patterns to be used by the system.

Each time the individual uses the system it will ask for a different biometric, maybe an index finger one time, and a middle finger the next. This would make it difficult for a potential spoofer because they would never know which biometric would be required for access.

IBG also says using multiple biometrics and multi-factor authentication, such as smart cards, could also prevent spoofing.

While there have been no documented cases of spoofing outside of the laboratory, vendors are not assuming they will not happen, given the increasing levels of technology available to hackers. To keep up, vendors must continue to improve the technology to keep ahead of the game. <

> Briefs, Page 3

software will be used to authenticate the identity of corrections employees entering and exiting facilities throughout the state, and provide attendance records. <

Precise, ActivCard Expand Partnership

Sweden-based Precise Biometrics, a fingerprint biometric systems vendor, and Fremont, Calif-based ActivCard, a digital ID card provider, expanded their partnership so the companies can deliver smart card-based ID badges with biometrics. ActivCard uses Precise's technology for matching biometric data on smart cards. The expanded partnership between the two will enable users to offer multi-factor authentication solutions that include a biometric credential. <

Facial Test Results Delayed

Results of the Facial Recognition Vendor Test might be delayed until February, according to a spokesperson at the National Institute of Standards and Technology. The FRVT 2002 is testing fourteen facial recognition systems in different settings. Results were supposed to be released in November, and then in December, but have been further delayed. <

IDNewswire
Trends in Personal Identification and Biometrics

Editor
Zack Martin
zachary.martin@thomsonmedia.com

Group Editor
Donald Davis
don.davis@thomsonmedia.com

Contributing Editor
Cathy Bowen
cathy.bowen@thomsonmedia.com

Advertising Sales
Jim Baker
james.baker@thomsonmedia.com

Publisher
Robert Jenisch
robert.jenisch@thomsonmedia.com

Group Publisher
Timothy Murphy
timothy.murphy@thomsonmedia.com

Thomson Media: *CEO: Robert Cullen; CFO: Roberto Rosati; Pres./CEO, Publishing & Conferences: Bruce Morris; SVP, Operations: Celie Baussan; CTO: Raymond Ouellette; VP, Business Development and Strategy: Greg Mazzanobile; VP, Finance: William Johnston; VP, Human Resources: Robert DeNoia.*

IDNewswire is published biweekly by Thomson Media. Visit our Web site at http://www.cardtechnology.com. The contents of IDNewswire are, and remain, the property of Thomson Media. Reproduction or forwarding of this publication is strictly prohibited. Individuals who infringe on these rights will be prosecuted to the full extent of the law.

Subscribers who want multiple copies of IDNewswire should contact Barbara Mahin at 212-803-8768 or barbara.mahin@thomsonmedia.com for information. The annual subscription rate is $695. For subscription, renewal or licensing information, please contact Barbara Mahin at 212-803-8768 or barbara.mahin@thomsonmedia.com.

For advertising information, contact Jim Baker at 312-983-6179 or james.baker@thomsonmedia.com. Editorial offices are located at 300 S. Wacker Drive, 18th Floor, Chicago, IL 60606. Telephone: 312-983-6168. FAX: 312-913-1365.

THOMSON™

Familiar Voice Unlocks A World of Different Services

By Kush Wadhwa
International Biometric Group

Are laptops, personal digital assistants, and Pocket PCs going to be replaced by the mobile phone?

This is the question being asked by many, including the strategists at Microsoft, who recently introduced a Windows-powered "smart phone." With mobile telephones now outnumbering fixed-line phones – in 2002 users of mobile phones exceeded 1 billion – it is fair to believe that users will expect increasingly greater value from these devices.

New smart phones will provide everything from color screens to built-in cameras. In addition to visual features, Samsung recent offerings provide built-in voice recognition and text-to-speech engines – foretelling the growth expected in voice-driven systems.

As customers require more complex operations, businesses face a daunting problem to secure such operations. Voice recognition technology, or VR, is helping to address these issues, using elements of both behavioral and physiological biometrics. VR technology uses the distinctiveness of an individual's voice, and combines that with how an individual speaks specific phrases or words in order to identify the individual.

For example, to enroll in a VR system, the user speaks a word or phrase, which is then converted from analog to digital format and transmitted for template generation. Subsequently, to authenticate the user, the same process is followed, with the newly generated template matched against the enrollment template.

In desktop-verification applications, a voice recognition engine may reside on a local or central PC, or may be Web-enabled. More commonly though, VR applications are being used with telephony-based systems. With these applications, the VR engine is either located on a central device at the institution with which the users are interacting, or is hosted by a third party.

Voice recognition technology is occasionally confused with speech recognition – a technology that translates what a user is saying. Leading vendors in the market, such as Nuance, Speechworks, and Voicevault, also sell speech recognition solutions, and frequently implement them in a complementary fashion. For example, VR technology may be used to validate a user to gain access to a telephony-based application, and speech recognition is used in order to translate spoken instructions into system operations or data inquiries.

As with most biometrics, the market for VR technology is growing rapidly, though current revenue levels are fairly low, estimated at $12.2 million for 2002. International Biometric Group projects that there will be a significant leap in adoption of this technology, driving the revenues up to $142 million by 2007, and growing its share of the biometric marketplace from current levels of 2.0% up to 3.5%.

VR systems are ripe for growth because they can leverage an existing, widespread, acquisition infrastructure – land telephones and mobile phones. Unlike other biometrics, growth of this technology is not dependent upon the distribution of proprietary acquisition devices.

In addition, implementation of such systems require no interruption or learning in existing user processes. For example, a user today may phone into a system and speak an account number or personal data or a PIN to gain access to information or initiate an operation. With VR, this process would not change, but would result in generation of enrollment templates, and upon subsequent access attempts, verification templates.

Today, many voice-based applications provide access to information. But as these services expand to allow access to more sensitive data, or to authorize financial transactions, companies and consumers will require higher levels of security – moving from speech recognition to VR biometrics. VR technology, combined with spoken phrases, particularly challenge phrases that might be considered "secret," such as a place of birth or residence, can provide the answer to these security requirements.

Beyond providing greater security, much of the motivation for implementing VR technology is linked to a desire to reduce call center costs. With even moderately accurate VR solutions capable of biometrically authenticating 80% to 90% of users, and routing 10% to 20% of callers through standard operator-based authentication processes, the result can be significantly lower call center costs. In addition, operators will be focused on screening the most suspect of callers, and increase their efforts at security.

Voice-Scan Strengths

- Leverages existing telephony infrastructure
- Requires little training or effort
- Certain solutions have very low false match rate
- Pass phrase can be changed – an advantage of behavioral biometrics

Voice-Scan Weaknesses

- Accuracy can be affected by illness
- Reduced performance with mobile phones
- Changing modes of enrollment and verification impacts accuracy
- Not a strong desktop solution
- Average user lacks confidence in technology

Bell Canada has recently implemented a system using VR and speech recognition technology to allow their field personnel to securely access and update customer installation and repair orders from any telephone. Beyond increasing mobility and convenience for their technicians, the company will reduce costs associated with equipping their technicians with notebook devices.

International Biometric Group

Even with these benefits, VR technology has not yet been widely deployed. This is likely to remain the case until the technology's accuracy and scalability has been confirmed by more substantial real-world experience. Scalability issues will be proven by deployment into incrementally larger production environments before new deployers will be likely to use VR in large-scale implementations.

Accuracy issues must be addressed to ensure that both institutions and their customers have confidence in the system. In International Biometric Group's Comparative Biometric Testing, certain VR systems have actually proven to be more resistant to spoofing attacks than some finger-scan systems.

On the other hand, many VR solutions can be susceptible to false non-matching, rejecting someone who is enrolled. Some of the issues are environmental, such as background noise, and telephone or signal quality. Some other reasons for false non-matching includes changes in a person's voice or speech habits. While consumers may be pleased to know that it is difficult for an imposter to gain access to their accounts, repeated non-match events will result in frustration with the system.

Telephony is the primary growth area for VR, with the largest opportunities in financial services account access. Such solutions often combine voice-scan with speech recognition, such that spoken account numbers are used to both retrieve personal data and verify identity.

Other leading applications include customer authentication for service calls and challenge-response implementations for house arrest and probation-related authentication. As an example, the recent implementation of VR technology for the U.S. District Court in South Florida is streamlining monitoring efforts for parolees and probationers on a weekly, monthly, and random basis.

While VR is a strong solution for implementations where voice-based interaction already exists, it is not currently expected to make an impact in situations where such interaction would be a new process.

In particular, PC-based VR is not to widespread, requiring certain technical issues be addressed: voice over Internet Protocol would need to be available, and microphones would need to be deployed at desktops. However, beyond these technical issues, the act of speaking to a computer would need to become more common before such applications are likely to take hold. <